IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

IN THE MATTER OF THE SEARCH OF A Samsung Galaxy cell phone #401-663-8946, model A51, black in color, that has a clear case, (hereinafter, "TARGET TELEPHONE 1"); and An Apple iPhone 13, cell phone #401-626-9662, model Pro Max, gold in color, (hereinafter, "TARGET TELEPHONE 2") CURRENTLY LOCATED AT 1162 Main St, West Warwick, RI 02893	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Tawnya Valdes, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following electronic devices – cell phones – which are currently in law enforcement possession and described in Attachments A-1 and A-2, and the extraction from that property of electronically stored information described in Attachment B:

   a. A Samsung Galaxy cell phone #401-663-8946, model A51, black in color, that has a clear case, (hereinafter, "TARGET TELEPHONE 1"); and

   b. An Apple iPhone 13, cell phone #401-626-9662, model Pro Max, gold in color, (hereinafter, "TARGET TELEPHONE 2"), (collectively, "the Devices").

2. TARGET TELEPHONE 1 was on MARTINEZ's person incident to his arrest on April 8, 2022. TARGET TELEPHONE 2 was located on PERALTA's person on April 8, 2022

incident to her arrest. PERALTA gave consent to officers to seize TARGET TELEPHONE 2 and provided her password.

3. The Devices are currently in the possession of West Warwick Police Department at 1162 Main St, West Warwick, RI 02893. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of law enforcement.

4. The applied-for warrants would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B, attached hereto, and incorporated herein.

5. As set forth below, there is probable cause to believe that located within the Devices are evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 641 (Theft of Government Funds); 42 U.S.C. § 1383a(a)(3) (False Statement); 18 U.S.C. § 1001(a)(1) (Scheme to Conceal Material Facts); and 18 U.S.C. § 2 (Aiding & Abetting), (collectively, the "Subject Offenses").

6. I am a member of the Social Security Administration's Office of the Inspector General ("SSA OIG") and am currently assigned to the Cooperative Disability Investigations ("CDI") Unit. Today, I am responsible for investigations involving allegations of fraud, waste, and abuse within SSA programs and benefits. I am currently assigned to conduct investigations in the Providence, RI office. I have worked for the SSA OIG for eight years and worked in the CDI unit for two years. Prior to my joining the SSA OIG and the CDI Unit, I worked for the Social Security Administration as a Claims Representative. I am a graduate of the Criminal

Investigator Training Program, and the Inspector General Investigator Training Program, at the Federal Law Enforcement Training Center at Glynco, Georgia.

7. I have authority to enforce the criminal laws of the United States and to make arrests. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

8. The facts in this affidavit come from my personal observations, my training and experience, evidence obtained from related investigations, and information or experience from other agents, law enforcement officers, and witnesses as well as public and law enforcement databases, public records, and an independent source of information. This affidavit is intended to show merely that there is probable cause for the requested search warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

Indictment and Arrests of MARTINEZ and PERALTA

9. On April 6, 2022, a grand jury returned an indictment of Daniel MARTINEZ and Daisy PERALTA. The Indictment alleges that MARTINEZ and PERALTA, as MARTINEZ's representative payee in the Social Security benefits program, received approximately $76,068 in Social Security Income, to which MARTINEZ was not entitled. I hereby incorporate by reference the allegations contained in the Indictment and submit that there is probable cause to believe that MARTINEZ and PERALTA defrauded the SSA by concealing MARTINEZ's ability to work, employment at and ownership of R&D Auto Sales, receipt of income and resources, change in physical condition, and change in living arrangements. *See* Exhibit A (22-cr-46).

10. On April 7, 2022, I participated in the arrest of PERALTA at her home. Incident to PERALTA's arrest, agents located TARGET TELEPHONE 2 on PERALTA's person. Subsequently, in the presence of her attorney, PERALTA signed a Consent to Search form for TARGET TELEPHONE 2. Therefore, while law enforcement agents might already have all necessary authority to examine TARGET TELEPHONE 2, I seek this additional warrant out of an abundance of caution to be certain that an examination of the device will comply with the Fourth Amendment and other applicable laws.

11. On April 8, 2022, MARTINEZ self-surrendered to the United States Marshals Service in response to learning about the warrant for his arrest in this case. MARTINEZ provided agents with TARGET TELEPHONE 1, which was found on MARTINEZ's person, at the U.S. Pastore Building during his arrest.

Electronic Evidence & Social Security Fraud

12. There is probable cause to believe that the Devices contain evidence, fruits, and instrumentalities of MARTINEZ's and PERALTA's Social Security fraud, theft of government money, and false statements. Based on my training and experience and discussions with other law enforcement officers who regularly investigate Social Security fraud offenses, I know that banking, financial, and business records of individuals and their companies are ordinarily kept for long periods of time, often for multiple years, and are not ordinarily destroyed.[1] Business

[1] See United States v. Farmer, 370 F.3d 435, 440 (4th Cir. 2004) (rejecting staleness argument and upholding finding of probable cause in part because the search warrant authorized agents to look for documents, including records of payment, bank statements, canceled checks, and check registers, which are "precisely the types of records that 'are not ordinarily destroyed or moved about from one place to another.'") (internal citations omitted); United States v. Aboud, 438 F.3d 554, at 573-74 (6th Cir. 2006) (observing that "business records are a type of evidence that defy claims of staleness"); see also United States v. Bosyk, 933 F.3d 319, 330–31 (4th Cir. Aug. 1,

owners maintain financial, customer, transactional, and other administrative records in electronic as well as physical format. I know based on my training and experience that in their digital devices, individuals maintain (among other items) bank records, loan records, records regarding the expenditure of money, records relating to the purchase of assets, records relating to the whereabouts and ownership of their residences, and records pertaining to their employment or business. These records constitute evidence, fruits, and instrumentalities of MARTINEZ's and PERALTA's Social Security fraud, theft of government money, and false statements.

13. Furthermore, in the course of this investigation, investigators learned of MARTINEZ's social media accounts and viewed MARTINEZ's various profiles on apps and websites, including Instagram and Facebook. From viewing MARTINEZ's various social media accounts, agents observed that MARTINEZ frequently posts photographs, videos, and messages that depict his physical condition and that are related to his work at R&D Auto Sales. Such public posts date as far back as 2013, and appear to be taken from MARTINEZ's cell phone as he conducts various physical activities, including driving a car, working at R&D Auto Sales, and walking around his home and the car business. The social media accounts also contain posts depicting MARTINEZ and PERALTA, including a video post from October 2020 where MARTINEZ discusses his business in front of PERALTA. Accordingly, there is probable cause to believe that the Devices contain evidence, fruits, and instrumentalities of the Subject Offenses involving MARTINEZ and PERALTA.

2019) (rejecting staleness challenge in a child pornography prosecution in part because relevant evidence is often electronically stored for long periods of time).

14. As described in the Indictment, PERALTA set up a custodial bank account for MARTINEZ at Bank of America, and she received and spent SSI program benefits from that account. After a cursory review of PERALTA's TARGET TELEPHONE 2 pursuant to her consent, investigators viewed a Bank of America app, as well as approximately nine (9) additional financial and banking apps. A witness, who is familiar with MARTINEZ's and PERALTA's activities as alleged in the Indictment, recently indicated that MARTINEZ conducted his business and personal banking through family members, including PERALTA, at Bank of America and other financial institutions previously unidentified by law enforcement. After reviewing previously subpoenaed Bank of America records of MARTINEZ's and PERALTA's bank accounts, agents subsequently confirmed that transfers, withdrawals, and other debits to various financial and banking institutions listed in TARGET TELEPHONE 2 do exist in MARTINEZ's and PERALTA's Bank of America records. Therefore, I believe that business and bank records related to the Subject Offenses exist within the Devices.

Digital Devices

15. The search warrant applications request the ability to search and seize information contained on digital devices.

16. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

17. Forensic methods may uncover electronic files or remnants of such file's months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may

only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

18. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

19. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

20. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

22. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

23. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

24. The search warrant applications request authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

25. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

26. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

27. Thus, the warrants I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrants: (1) depress MARTINEZ's and/or PERALTA's thumbs- and/or fingers on the device(s); and (2) hold the device(s) in front of MARTINEZ's and/or PERALTA's face(s) with his/her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

28. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means

Electronic Storage and Forensic Analysis

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the device

consistent with the warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrants.

32. *Manner of execution.* Because these warrants seek only permission to examine a device already in law enforcement's possession, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

33. Based on the aforementioned information, your affiant prays that search warrants be issued in order to search the Devices by a member of the SSA OIG, a member of the Rhode Island State Police Computer Crimes Unit, and/or a member or qualified designee from a law enforcement agency and/or a member or designee of a federal law enforcement agency for any and all evidence related to the Subject Offenses. Furthermore, your affiant requests that a member of the above-referenced law enforcement groups be allowed to conduct an off-site forensic analysis of the seized mobile device to fully develop the link between MARTINEZ, and PERALTA, along with anyone else involved in the Subject Offenses.

CONCLUSION

34. Based upon the facts set forth above, I believe that there is probable cause to believe that the Devices, as described in Attachments A-1 and A-2, contain evidence of the Subject Offenses. As described above and in Attachment B, this application seeks permission to search and seize things that the Devices might contain relating to Subject Offenses, in whatever form they are stored. For all of the foregoing reasons, I respectfully request that this Court issue the requested search warrants.

I declare that the foregoing is true and correct.

Tawnya Valdes, SSA OIG

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone.

(*Specify reliable electronic means)*

_____	_____
Date	*Judge's signature*
_____	_____
City and State	*U.S. Magistrate Judge*

ATTACHMENT A-1

(Description of Property to be searched)

A Samsung Galaxy cell phone #401-663-8946, model A51, black in color, that has a clear case, (hereinafter, "TARGET TELEPHONE 1)

ATTACHMENT A-2

(Description of Property to be searched)

An Apple iPhone 13, cell phone #401-626-9662, model Pro Max, gold in color, (hereinafter, "TARGET TELEPHONE 2")

ATTACHMENT B

(Items to be seized)

Evidence or instrumentalities of violations of evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 641 (Theft of Government Funds); 42 U.S.C. § 1383a(a)(3) (False Statement); 18 U.S.C. § 1001(a)(1) (Scheme to Conceal Material Facts); and 18 U.S.C. § 2 (Aiding & Abetting), (collectively, the "Subject Offenses"), including, without limitation, records relating to:

Records and information,[2] including the following:

1. Call logs.

2. Address books, contact names.

3. Incoming call history; Outgoing call history; Missed call history; Outgoing text messages; Incoming text messages; Draft text messages; Voice Mails.

4. Data screen or file identifying the telephone number associated with the mobile telephone searched and serial numbers or other information to identify with the mobile telephone searched.

5. User-entered messages (such as to-do lists).

6. Any passwords used to access the electronic data described herein.

7. Text messages, SMS messages, MMS messages, social media messages (including but not limited to Instagram messages, Facebook messages, and WhatsApp messages), emails, or other communication forms among associates, known and unknown, including but not limited to MARTINEZ and PERALTA, concerning MARTINEZ's physical condition, income and resources, living arrangements, ability to work or hold employment, receipt of public benefits, and scope of ownership of and employment at R&D Auto Sales.

8. Evidence of user attribution showing who used or owned the Devices at the time the things described in these warrants were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords and browsing history, and documents.

---

[2] As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

9. Internet searches and history.

10. GPS search histories.

11. Records showing use of phone applications for communications and other user accounts for applications, email, and other internet and app-based accounts.

12. Photographs or video of MARTINEZ, PERALTA, and others known and unknown, and photographs depicting or regarding MARTINEZ's medical condition, income and resources, place of residence, ability to work or hold employment, receipt of public benefits, and scope of ownership of and employment at R&D Auto Sales, to include any metadata showing the GPS coordinates where the photographs or video images were created.

13. All records and information, including but not limited to business and financial records, concerning MARTINEZ's medical condition, income and resources, living arrangements, ability to work or hold employment, receipt of public benefits, and scope of ownership of and employment at R&D Auto Sales.

14. All communications between MARTINEZ and PERALTA regarding medical condition, income and resources, place of residence, ability to work or hold employment, receipt of SSA benefits, and ownership of and employment at R&D Auto Sales.

15. General ledgers, cash receipts journals, cash disbursement journals, petty cash journals, bank statements, passbooks, cancelled checks, check stubs or registers, deposit tickets, deposit receipts, cashier's checks, money orders, wire transfer documents, invoices, written estimates, receipts, contracts, agreements, customer ledger cards, purchases journals, advance payment ledgers, accounts payable ledgers, accounts receivable ledgers, correspondence, memoranda and documents.

16. Records of income and expenses, such as profit and loss statements, financial statements, balance sheets and income and expense journals.

17. Bank records, including but not limited to cancelled checks, cashier's checks, money orders, statements, deposit tickets, and withdrawal slips.

18. Records of loans, whether or not the loan was received, to include but not limited to loan applications or agreements, credit checks, reference checks, copies of notes or mortgages, and repayment records.

19. Records pertaining to the rental of safe deposit boxes and corresponding keys.

20. Tax records, statements and returns.

21. Travel records, to include books, records, receipts, notes, ledgers, airline ticket, vehicle rental receipts, credit card receipts and bills, hotel receipts, meal receipts, travel agency vouchers, travel schedules or other travel-related papers.

22. Records of deeds, mortgages, leases, escrow accounts and utility billings including evidence of dominion control of property.

23. Records or information, including but not limited to contracts and other agreements, reflecting associations between individuals relative to business ventures.

24. Records evidencing the obtaining, secreting, transfer, concealment, transfer or expenditure of money, United States currency, papers, and identification documents, whether kept manually and/or by mechanical, and/or electronic devices pertaining to the wiring and/or receipt of funds.

25. Documents pertaining to purchase of assets to include but not limited to: investments, precious metals, automobiles, jewelry, household furniture and appliances.

26. Records of personal or business activities relating to the operation or ownership of any computer hardware, software, storage media, or data (such as user names, passwords, telephone records, notes, books, diaries, and reference materials).

27. Records relating to ownership, occupancy, or use of the R&D Auto Sales (such as utility bills, phone bills, rent payments, mortgage payments, business ledgers, car auction records, photographs, insurance documentation, receipts and check registers).

28. Records relating to the receipt of social security benefits, to include but not be limited to, correspondence from the Social Security Administration.

It is specifically requested that the searching agents or officers be authorized to answer and record all telephone calls received on the Devices to be searched during the execution of the search warrant and to record and return any incoming pages or text messages received during the execution of these search warrants.

During the execution of these search warrants, law enforcement is permitted to:

> **(1) depress the thumb- and/or fingers of Daniel MARTINEZ and/or DAISY PERALTA on the device(s); and**
> **(2) hold the device(s) in front of the faces of Daniel MARTINEZ and/or DAISY PERALTA with his/her eyes open to activate the facial-, iris-, and/or retina-recognition feature**

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor,

490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.